HALTON-TYPE SEQUENCES FROM GLOBAL FUNCTION FIELDS

HARALD NIEDERREITER AND ANDERSON SIANG JING YEO

ABSTRACT. For any prime power q and any dimension $s \geqslant 1$, a new construction of (t, s)-sequences in base q using global function fields is presented. The construction yields an analog of Halton sequences for global function fields. It is the first general construction of (t, s)-sequences that is not based on the digital method. The construction can also be put into the framework of the theory of $(u, \mathbf{e}, s)$-sequences that was recently introduced by Tezuka and leads in this way to better discrepancy bounds for the constructed sequences.

1. INTRODUCTION

The construction of low-discrepancy sequences is an important problem in number theory and combinatorics and it is also highly relevant for quasi-Monte Carlo methods in scientific computing (see [2, 9]). Let us recall the definition of the star discrepancy and the associated definition of a low-discrepancy sequence. Let $s \geqslant 1$ be a given dimension and let $\mathcal{P}$ be a point set consisting of the N points $\mathbf{x}_0, \ldots, \mathbf{x}_{N-1}$ in the s-dimensional unit cube $[0, 1]^s$. For a subinterval J of $[0, 1]^s$, let $A(J; \mathcal{P})$ be the number of integers n with $0 \leqslant n \leqslant N - 1$ and $\mathbf{x}_n \in J$. Then the *star discrepancy* $D_N^*(\mathcal{P})$ of $\mathcal{P}$ is defined by

$$D_N^*(\mathcal{P}) = \sup_J \left| \frac{A(J; \mathcal{P})}{N} - \lambda_s(J) \right|,$$

where the supremum is extended over all subintervals J of $[0, 1]^s$ with one vertex at the origin and λ_s denotes the s-dimensional Lebesgue measure. For a sequence $\mathcal{S}$ of points $\mathbf{x}_0, \mathbf{x}_1, \ldots$ in $[0, 1]^s$, we define the star discrepancy $D_N^*(\mathcal{S})$ for all $N \geqslant 1$ by putting $D_N^*(\mathcal{S}) = D_N^*(\mathcal{P}_N)$, where $\mathcal{P}_N$ is the point set consisting of the first N terms $\mathbf{x}_0, \ldots, \mathbf{x}_{N-1}$ of $\mathcal{S}$. We say that $\mathcal{S}$ is a *low-discrepancy sequence* if

$$(1) \qquad\qquad D_N^*(\mathcal{S}) = O(N^{-1}(\log N)^s) \qquad \text{for all } N \geqslant 2,$$

where the implied constant is independent of N. This is the smallest possible order of magnitude that can currently be obtained for the star discrepancy of a sequence of points in $[0, 1]^s$. Actually, it is a widely held belief that no smaller order of magnitude can be achieved.

Historically, the first construction of low-discrepancy sequences for any dimension was that of Halton sequences in [4]. For any integer $b \geqslant 2$, let $Z_b = \{0, 1, \ldots, b - 1\} \subset \mathbb{Z}$ denote the least residue system modulo b. Every integer $n \geqslant 0$ has a unique digit expansion

$$n = \sum_{r=0}^{\infty} a_r(n) b^r$$

in base b, where $a_r(n) \in Z_b$ for all $r \geqslant 0$ and $a_r(n) = 0$ for all sufficiently large r. The *radical-inverse function* ϕ_b in base b is defined by

$$\phi_b(n) = \sum_{r=0}^{\infty} a_r(n) b^{-r-1} \in [0, 1) \qquad \text{for all } n \in \mathbb{N}_0.$$

As usual, we write $\mathbb{N}_0$ for the set of nonnegative integers and $\mathbb{N}$ for the set of positive integers. Now choose pairwise coprime integers $b_1, \ldots, b_s \geqslant 2$ and define the *Halton sequence in the*

bases $b_1, \ldots, b_s$ as the sequence $\mathbf{h}_0, \mathbf{h}_1, \ldots$ with

$$\mathbf{h}_n = (\phi_{b_1}(n), \ldots, \phi_{b_s}(n)) \in [0, 1)^s \qquad \text{for } n = 0, 1, \ldots.$$

An explicit upper bound of the form (1) for the star discrepancy of this Halton sequence can be found in [2, Theorem 3.36]. In practical implementations, the bases $b_1, \ldots, b_s$ are usually taken to be distinct prime numbers.

Modern methods for the construction of s-dimensional low-discrepancy sequences are based on the theory of (t, m, s)-nets and (t, s)-sequences which was developed in [7]. This theory has a strong combinatorial flavor; see [2, Chapter 6], [9, Chapter 4], and the article on (t, m, s)-nets in the handbook [1]. The currently most powerful constructions of (t, s)-sequences use global function fields and quite a number of such constructions are available; see [5, 6, 10, 11, 12, 19] as well as the surveys in [2, 13, 14, 15].

In this paper we present a new construction of low-discrepancy sequences using global function fields. The construction is comparatively simple and inspired by the construction of Halton sequences. It fits very well into the framework of the theory of $(u, \mathbf{e}, s)$-sequences developed recently by Tezuka [18]. This theory is an extension of the theory of (t, s)-sequences and leads in many cases to better upper bounds on the star discrepancy. The new construction is exceptional in the sense that it is the first general construction of (t, s)-sequences and $(u, \mathbf{e}, s)$-sequences that is not based on the digital method, which so far was the standard method of constructing (t, s)-sequences and $(u, \mathbf{e}, s)$-sequences (see [2, Chapter 4] for a description of the digital method). Rather, our construction provides a direct and explicit formula for the terms of the sequence (see equation (7) in Section 3).

The rest of the paper is organized as follows. In Section 2 we present the necessary background on $(u, \mathbf{e}, s)$-sequences. Section 3 contains the construction of our Halton-type sequences. In Section 4 we show that these sequences are both $(u, \mathbf{e}, s)$-sequences and (t, s)-sequences with suitable parameters u, $\mathbf{e}$, and t. Upper bounds on the star discrepancy of these sequences are discussed in Section 5.

2. Background on $(u, \mathbf{e}, s)$-sequences

Tezuka [18] recently introduced the concepts of $(u, m, \mathbf{e}, s)$-nets and $(u, \mathbf{e}, s)$-sequences. For several reasons, e.g., to prove Proposition 1 below and to avoid unnecessary additional conditions, his definitions were slightly revised by Hofer and Niederreiter [5]. We follow this revised approach.

Definition 1. Let $b \geqslant 2$, $s \geqslant 1$, and $0 \leqslant u \leqslant m$ be integers and let $\mathbf{e} = (e_1, \ldots, e_s) \in \mathbb{N}^s$ be an s-tuple of positive integers. A $(u, m, \mathbf{e}, s)$-*net in base* b is a point set $\mathcal{P}$ of b^m points in $[0, 1)^s$ such that $A(J; \mathcal{P}) = b^m \lambda_s(J)$ for every interval J of the form

$$(2) \qquad\qquad J = \prod_{i=1}^{s} \left[a_i b^{-d_i}, (a_i + 1) b^{-d_i} \right)$$

with integers $d_i \geqslant 0$, $0 \leqslant a_i < b^{d_i}$, and $e_i | d_i$ for $1 \leqslant i \leqslant s$ and with $\lambda_s(J) \geqslant b^{u-m}$.

The classical concept of a (u, m, s)-net in base b corresponds to the special case $\mathbf{e} = (1, \ldots, 1)$ in Definition 1. For a real number $x \in [0, 1]$, let

$$x = \sum_{j=1}^{\infty} y_j b^{-j} \qquad \text{with all } y_j \in Z_b$$

be a b-adic expansion of x, where the case $y_j = b - 1$ for all sufficiently large j is allowed. For any integer $m \geqslant 1$, we define the truncation

$$[x]_{b,m} = \sum_{j=1}^{m} y_j b^{-j}.$$

If $\mathbf{x} = (x^{(1)}, \ldots, x^{(s)}) \in [0,1]^s$, then the truncation $[\mathbf{x}]_{b,m}$ is defined coordinatewise, that is,

$$[\mathbf{x}]_{b,m} = \left([x^{(1)}]_{b,m}, \ldots, [x^{(s)}]_{b,m}\right).$$

Definition 2. Let $b \geqslant 2$, $s \geqslant 1$, and $u \geqslant 0$ be integers and let $\mathbf{e} \in \mathbb{N}^s$. A sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ of points in $[0,1]^s$ is called a $(u, \mathbf{e}, s)$-*sequence in base* b if for all integers $k \geqslant 0$ and $m > u$ the points $[\mathbf{x}_n]_{b,m}$ with $kb^m \leqslant n < (k+1)b^m$ form a $(u, m, \mathbf{e}, s)$-net in base b.

The classical concept of a (u, s)-sequence in base b corresponds to the special case $\mathbf{e} = (1, \ldots, 1)$ in Definition 2. The following result was shown in [5].

Proposition 1. *Let $b \geqslant 2$, $s \geqslant 1$, and $u \geqslant 0$ be integers and let $\mathbf{e} = (e_1, \ldots, e_s) \in \mathbb{N}^s$. Then any $(u, \mathbf{e}, s)$-sequence in base b is a (t, s)-sequence in base b with*

$$t = u + \sum_{i=1}^{s} (e_i - 1).$$

For $\mathbf{e} \neq (1, \ldots, 1)$, there are currently four families of sequences for which it has been verified that they are $(u, \mathbf{e}, s)$-sequences: the Niederreiter sequences constructed in [8], the generalized Niederreiter sequences constructed in [17], the Niederreiter-Xing sequences constructed in [19], and the Hofer-Niederreiter sequences constructed in [5]. The proof of the property of being $(u, \mathbf{e}, s)$-sequences is given in [18] for Niederreiter sequences and generalized Niederreiter sequences and in [5] for Niederreiter-Xing sequences and Hofer-Niederreiter sequences.

3. The construction

As we have already mentioned, our new construction of low-discrepancy sequences is based on global function fields. Recall that a *global function field* is an algebraic function field of one variable over a finite field. We follow the monograph [16] regarding terminology and notation for global function fields.

We write $\mathbb{F}_q$ for the finite field with q elements, where q is an arbitrary prime power. Let F be a global function field with full constant field $\mathbb{F}_q$, that is, with $\mathbb{F}_q$ algebraically closed in F. We assume that F has at least one rational place, that is, a place of degree 1. Given a dimension $s \geqslant 1$, we choose $s+1$ distinct places $P_\infty, P_1, \ldots, P_s$ of F with $\deg(P_\infty) = 1$. The degrees of the places $P_1, \ldots, P_s$ are arbitrary and we put $e_i = \deg(P_i)$ for $1 \leqslant i \leqslant s$. Denote by O_F the holomorphy ring given by

$$O_F = \bigcap_{P \neq P_\infty} O_P,$$

where the intersection is extended over all places $P \neq P_\infty$ of F and O_P is the valuation ring of P. For each $i = 1, \ldots, s$, let $\wp_i$ be the maximal ideal of O_F corresponding to P_i. Then the residue class field $F_{P_i} := O_F/\wp_i$ has order q^{e_i} (see [16, Proposition 3.2.9]). We fix a bijection

$$(3) \qquad\qquad\qquad \sigma_{P_i} : F_{P_i} \to Z_{q^{e_i}}.$$

For any divisor D of F, we write $\mathcal{L}(D)$ for the Riemann-Roch space associated to D and $\ell(D)$ for the dimension of the vector space $\mathcal{L}(D)$ over $\mathbb{F}_q$ (see [16, Section 1.4]). For each $i = 1, \ldots, s$, we can obtain a local parameter $z_i \in O_F$ at $\wp_i$, by applying the Riemann-Roch theorem [16, Theorem 1.5.17] and choosing

$$z_i \in \mathcal{L}(kP_\infty - P_i) \setminus \mathcal{L}(kP_\infty - 2P_i)$$

for a suitably large integer k. Then for every $f \in O_F$, we have a local expansion of f at $\wp_i$ of the form

$$(4) \qquad\qquad\qquad f = \sum_{j=0}^{\infty} f_{i,j} z_i^j \qquad \text{with all } f_{i,j} \in F_{P_i}.$$

Compare with [15, pp. 5–6] for a detailed description of how to obtain a local expansion. Now we define the map $\phi : O_F \to [0,1]^s$ by

$$(5) \qquad \phi(f) = \left(\sum_{j=0}^{\infty} \sigma_{P_1}(f_{1,j})(q^{e_1})^{-j-1}, \ldots, \sum_{j=0}^{\infty} \sigma_{P_s}(f_{s,j})(q^{e_s})^{-j-1} \right) \qquad \text{for all } f \in O_F.$$

The map ϕ can be viewed as an s-dimensional radical-inverse function for O_F.

We arrange the elements of O_F into a sequence by using the fact that

$$O_F = \bigcup_{m=0}^{\infty} \mathcal{L}(mP_\infty).$$

The terms of this sequence are denoted by $f_0, f_1, \ldots$ and they are obtained as follows. Consider the chain

$$\mathcal{L}(0) \subseteq \mathcal{L}(P_\infty) \subseteq \mathcal{L}(2P_\infty) \subseteq \cdots$$

of vector spaces over $\mathbb{F}_q$. At each step of this chain, the dimension either remains the same or increases by 1. From a certain point on, the dimension always increases by 1 according to the Riemann-Roch theorem. Thus, we can construct a sequence $v_0, v_1, \ldots$ of elements of O_F such that for each $m \in \mathbb{N}_0$,

$$\{v_0, v_1, \ldots, v_{\ell(mP_\infty)-1}\}$$

is an $\mathbb{F}_q$-basis of $\mathcal{L}(mP_\infty)$. For $n \in \mathbb{N}_0$, let

$$n = \sum_{r=0}^{\infty} a_r(n)q^r \qquad \text{with all } a_r(n) \in Z_q$$

be the digit expansion of n in base q. Note that $a_r(n) = 0$ for all sufficiently large r. We fix a bijection $\eta : Z_q \to \mathbb{F}_q$ with $\eta(0) = 0$. Then we define

$$(6) \qquad f_n = \sum_{r=0}^{\infty} \eta(a_r(n))v_r \in O_F \qquad \text{for } n = 0, 1, \ldots.$$

Note that the sum above is finite since for each $n \in \mathbb{N}_0$ we have $\eta(a_r(n)) = 0$ for all sufficiently large r.

Using (5) and (6), we now define the sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ of points in $[0,1]^s$ by

$$(7) \qquad \mathbf{x}_n = \phi(f_n) \qquad \text{for } n = 0, 1, \ldots.$$

This is our Halton-type sequence obtained from the global function field F. We will show that this sequence is a $(u, \mathbf{e}, s)$-sequence in base q for some u and $\mathbf{e}$ (see Theorem 1 below) and also a (t, s)-sequence in base q for some t (see Corollary 1 below).

Remark 1. The sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ is obtained by the direct and explicit formula (7) and it is easy to see that, in general, it cannot be produced by the digital method for the construction of (t, s)-sequences. The simple reason is that the digital method for the construction of (t, s)-sequences in base q is a linear-algebra technique which works entirely in the finite field $\mathbb{F}_q$ (compare again with [2, Chapter 4]), whereas our construction uses extension fields of $\mathbb{F}_q$ of degrees $e_1, \ldots, e_s$. Moreover, whenever $e_i \geqslant 2$ there is no reasonable way in which the bijection σ_{P_i} in (3) can be interpreted as an $\mathbb{F}_q$-linear map. There is only one situation in which our construction can be put into the framework of the digital method, namely when q is a prime number and $e_i = 1$ for $1 \leqslant i \leqslant s$. In this case the bijections σ_{P_i} in (3) can be chosen as identity maps.

Remark 2. Tezuka [17] introduced a construction of Halton-type sequences based on rational function fields over finite fields. If we specialize our construction to the case where F is the rational function field over $\mathbb{F}_q$, then our construction is in general different from Tezuka's construction. One significant difference is that Tezuka's construction can be described in

terms of the digital method, whereas our construction cannot in general be put into the framework of the digital method (see Remark 1).

4. THE MAIN RESULT

Before we formulate our main result in Theorem 1 below, we prove the following lemma. We keep the notation from the previous sections.

Lemma 1. *Let g be the genus of F and let $k \geqslant 0$ and $m \geqslant g$ be integers. Let the elements $f_n \in O_F$ be defined by (6). Then for $f \in O_F$ we have $f = f_n$ for some integer n with $kq^m \leqslant n < (k+1)q^m$ if and only if $f = h + c$ with $h \in O_F$ depending only on k and m and with $c \in \mathcal{L}((m + g - 1)P_\infty)$.*

Proof. The integers n with $kq^m \leqslant n < (k+1)q^m$ have digit expansions in base q of the form

$$n = \sum_{r=0}^{m-1} a_r(n) q^r + \sum_{r=m}^{\infty} a_r(n) q^r,$$

where the $a_r(n)$ with $0 \leqslant r \leqslant m - 1$ range independently over Z_q and the $a_r(n)$ with $r \geqslant m$ depend only on k. Thus, the corresponding f_n have the form

$$(8) \qquad f_n = \sum_{r=0}^{m-1} \eta(a_r(n)) v_r + \sum_{r=m}^{\infty} \eta(a_r(n)) v_r =: \sum_{r=0}^{m-1} \alpha_r v_r + h,$$

where the $\alpha_r = \eta(a_r(n))$ with $0 \leqslant r \leqslant m - 1$ range independently over $\mathbb{F}_q$ and $h \in O_F$ depends only on k and m.

Now we consider $\mathcal{L}((m + g - 1)P_\infty)$ and note that $\deg((m + g - 1)P_\infty) = m + g - 1 \geqslant 2g - 1$. Therefore $\ell((m + g - 1)P_\infty) = m$ by the Riemann-Roch theorem. It follows that $\{v_0, v_1, \ldots, v_{m-1}\}$ is an $\mathbb{F}_q$-basis of $\mathcal{L}((m + g - 1)P_\infty)$, and so the linear combinations $\sum_{r=0}^{m-1} \alpha_r v_r$ range exactly over $\mathcal{L}((m + g - 1)P_\infty)$. In view of (8), the proof is complete. □

Theorem 1. *The sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ given by (7) is a $(u, \mathbf{e}, s)$-sequence in base q with $u = g$ and $\mathbf{e} = (e_1, \ldots, e_s)$, where g is the genus of F and $e_i = \deg(P_i)$ for $1 \leqslant i \leqslant s$.*

Proof. We proceed by Definition 2 and fix integers $k \geqslant 0$ and $m > g$. We have to show that the point set $\mathcal{P}_{k,m}$ consisting of the points $[\mathbf{x}_n]_{q,m} = [\phi(f_n)]_{q,m}$ with $kq^m \leqslant n < (k+1)q^m$ forms a $(g, m, \mathbf{e}, s)$-net in base q.

Let J be an interval of the form (2) with $\lambda_s(J) \geqslant q^{g-m}$, that is,

$$(9) \qquad \sum_{i=1}^{s} d_i \leqslant m - g.$$

Note that we assume $e_i | d_i$ for $1 \leqslant i \leqslant s$ according to Definition 1. Let $f \in O_F$ with local expansions as in (4). Then $[\phi(f)]_{q,m} \in J$ if and only if

$$\left[\sum_{j=1}^{\infty} \sigma_{P_i}(f_{i,j-1}) (q^{e_i})^{-j} \right]_{q,m} \in [a_i q^{-d_i}, (a_i + 1) q^{-d_i}) \qquad \text{for } 1 \leqslant i \leqslant s.$$

This is equivalent to

$$w_i := \sum_{j=1}^{d_i/e_i} \sigma_{P_i}(f_{i,j-1}) q^{-je_i} \in [a_i q^{-d_i}, (a_i + 1) q^{-d_i}) \qquad \text{for } 1 \leqslant i \leqslant s.$$

This condition is satisfied if and only if, for $1 \leqslant i \leqslant s$, the first d_i q-adic digits of w_i agree with the first d_i q-adic digits of $a_i q^{-d_i}$ and thus have fixed values depending only on J. Note

that these d_i fixed q-adic digits of w_i correspond to d_i/e_i fixed q^{e_i}-adic digits. Therefore for some $a_{i,j} \in Z_{q^{e_i}}$, $1 \leqslant j \leqslant d_i/e_i$, $1 \leqslant i \leqslant s$, we get the condition

$$\sigma_{P_i}(f_{i,j-1}) = a_{i,j} \qquad \text{for } 1 \leqslant j \leqslant d_i/e_i, \ 1 \leqslant i \leqslant s,$$

or the equivalent condition

$$(10) \qquad\qquad f_{i,j-1} = \sigma_{P_i}^{-1}(a_{i,j}) =: \beta_{i,j} \in F_{P_i} \qquad \text{for } 1 \leqslant j \leqslant d_i/e_i, \ 1 \leqslant i \leqslant s.$$

Now we recall (4) and put

$$h_i = \sum_{j=0}^{(d_i/e_i)-1} \beta_{i,j+1} z_i^j \in O_F \qquad \text{for } 1 \leqslant i \leqslant s.$$

Then (10) is equivalent to

$$(11) \qquad\qquad f \equiv h_i \bmod \wp_i^{d_i/e_i} \qquad \text{for } 1 \leqslant i \leqslant s.$$

Note that the elements $h_1, \ldots, h_s$ depend only on J.

We consider now the number $A(J; \mathcal{P}_{k,m})$ of integers n with $kq^m \leqslant n < (k+1)q^m$ such that $[\phi(f_n)]_{q,m} \in J$. As we have just seen, the latter condition is equivalent to (11) holding for $f = f_n$. By Lemma 1 the condition $kq^m \leqslant n < (k+1)q^m$ is equivalent to $f_n = h + c$ with fixed $h \in O_F$ and some $c \in \mathcal{L}((m+g-1)P_\infty)$. Thus, both conditions hold simultaneously if and only if $c \in \mathcal{L}((m+g-1)P_\infty)$ satisfies

$$(12) \qquad\qquad c \equiv h_i - h \bmod \wp_i^{d_i/e_i} \qquad \text{for } 1 \leqslant i \leqslant s.$$

Consider the map

$$\psi : \mathcal{L}((m+g-1)P_\infty) \to R := (O_F/\wp_1^{d_1/e_1}) \times \cdots \times (O_F/\wp_s^{d_s/e_s})$$

defined by

$$\psi(c) = (c \bmod \wp_1^{d_1/e_1}, \ldots, c \bmod \wp_s^{d_s/e_s}) \qquad \text{for } c \in \mathcal{L}((m+g-1)P_\infty).$$

Note that ψ is a linear transformation between vector spaces over $\mathbb{F}_q$. We claim that ψ is surjective. To prove this, it suffices to show that

$$\dim(\mathcal{L}((m+g-1)P_\infty)/\ker(\psi)) = \dim(R).$$

The dimension $\dim(R)$ is easily computed to be

$$\dim(R) = \sum_{i=1}^{s} \dim(O_F/\wp_i^{d_i/e_i}) = \sum_{i=1}^{s} d_i.$$

From the definition of ψ it is clear that

$$(13) \qquad\qquad \ker(\psi) = \mathcal{L}\Big((m+g-1)P_\infty - \sum_{i=1}^{s}(d_i/e_i)P_i\Big).$$

Furthermore, by taking into account (9) we get

$$(14) \qquad \deg\Big((m+g-1)P_\infty - \sum_{i=1}^{s}(d_i/e_i)P_i\Big) = m+g-1 - \sum_{i=1}^{s} d_i \geqslant 2g-1.$$

Therefore

$$\dim(\mathcal{L}((m+g-1)P_\infty)/\ker(\psi)) = \dim\Big(\mathcal{L}((m+g-1)P_\infty)/\mathcal{L}\Big((m+g-1)P_\infty - \sum_{i=1}^{s}(d_i/e_i)P_i\Big)\Big)$$

$$= \deg\Big(\sum_{i=1}^{s}(d_i/e_i)P_i\Big) = \sum_{i=1}^{s} d_i$$

by the Riemann-Roch theorem, and so ψ is indeed surjective.

Since ψ is surjective, the number of $c \in \mathcal{L}((m + g - 1)P_\infty)$ satisfying the system of congruences in (12) is equal to $\# \ker(\psi)$. By (13), (14), and the Riemann-Roch theorem we get

$$
\begin{aligned}
\dim(\ker(\psi)) &= \ell\Big((m + g - 1)P_\infty - \sum_{i=1}^{s}(d_i/e_i)P_i\Big) \\
&= \deg\Big((m + g - 1)P_\infty - \sum_{i=1}^{s}(d_i/e_i)P_i\Big) + 1 - g = m - \sum_{i=1}^{s}d_i.
\end{aligned}
$$

Thus, we have shown that

$$
A(J; \mathcal{P}_{k,m}) = \# \ker(\psi) = q^{m - \sum_{i=1}^{s} d_i}.
$$

On the other hand, we have

$$
q^m \lambda_s(J) = q^{m - \sum_{i=1}^{s} d_i}
$$

by the form of J, and so $\mathcal{P}_{k,m}$ is indeed a $(g, m, \mathbf{e}, s)$-net in base q according to Definition 1. $\qquad\square$

Corollary 1. *The sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ given by (7) is a (t, s)-sequence in base q with*

$$
t = g + \sum_{i=1}^{s}(e_i - 1),
$$

where g is the genus of F and $e_i = \deg(P_i)$ for $1 \leqslant i \leqslant s$.

Proof. This follows from Theorem 1 and Proposition 1. $\qquad\square$

Remark 3. The Niederreiter-Xing sequences constructed in [19] use the same ingredients as our construction, to wit a global function field F with full constant field $\mathbb{F}_q$ and $s+1$ distinct places $P_\infty, P_1, \ldots, P_s$ of F with $\deg(P_\infty) = 1$ and the degrees $e_i = \deg(P_i)$ for $1 \leqslant i \leqslant s$ being arbitrary. It was shown in [19] that a Niederreiter-Xing sequence with these data is a (t, s)-sequence in base q with the same value of t as in Corollary 1. Furthermore, Hofer and Niederreiter [5] proved that the same Niederreiter-Xing sequence is also a $(g, \mathbf{e}, s)$-sequence in base q with $\mathbf{e} = (e_1, \ldots, e_s)$, that is, with the same parameters as in Theorem 1. Thus, the Niederreiter-Xing sequence and our new Halton-type sequence have a similar distribution behavior. However, it should be pointed out that our new construction is considerably simpler than the one in [19]. Since the Niederreiter-Xing sequences and our new Halton-type sequences have the same parameters, the usual procedure of optimizing the t-value for Niederreiter-Xing sequences (see [12] and [15, Section 8.3]) applies in the same way to our new Halton-type sequences. Consequently, our new construction yields (t, s)-sequences in base q such that, for fixed q, the parameter t grows linearly in s as $s \to \infty$ and is therefore asymptotically optimal.

5. DISCREPANCY BOUNDS

The star discrepancy $D_N^*(\mathcal{S})$ of any (t, s)-sequence $\mathcal{S}$ in any base $b \geqslant 2$ satisfies an upper bound of the form (1). In fact, we have

$$
(15) \qquad D_N^*(\mathcal{S}) \leqslant C N^{-1}(\log N)^s + O(N^{-1}(\log N)^{s-1}) \qquad \text{for all } N \geqslant 2
$$

with the constant $C > 0$ and the implied constant in the Landau symbol depending only on b, s, and t. This was first shown in [7, Section 4] (see also [9, Theorem 4.17] for a convenient formulation). The currently best values of C are those of Faure and Kritzer [3], namely $C = C_{\mathrm{FK}}$ given by

$$
C_{\mathrm{FK}} = \begin{cases} \dfrac{b^t}{s!} \cdot \dfrac{b^2}{2(b^2-1)}\left(\dfrac{b-1}{2\log b}\right)^s & \text{if } b \text{ is even,} \\[2ex] \dfrac{b^t}{s!} \cdot \dfrac{1}{2}\left(\dfrac{b-1}{2\log b}\right)^s & \text{if } b \text{ is odd.} \end{cases}
$$

It follows that for every base $b \geqslant 2$ we have

$$(16) \qquad C_{\text{FK}} \geqslant \frac{b^t}{s!} \cdot \frac{1}{2} \left(\frac{b-1}{2 \log b} \right)^s .$$

Tezuka [18] established an upper bound on the star discrepancy $D_N^*(\mathcal{S})$ of any $(u, \mathbf{e}, s)$-sequence $\mathcal{S}$ in base b. This bound is also of the form (15) with the constant $C = C_{\text{Tez}}$ given by

$$(17) \qquad C_{\text{Tez}} = \frac{b^u}{s!} \prod_{i=1}^{s} \frac{\lfloor b^{e_i}/2 \rfloor}{e_i \log b} \leqslant \frac{b^u}{s!} \cdot \frac{b^{e_1 + \cdots + e_s}}{(2 \log b)^s e_1 \cdots e_s} .$$

Note that our Definition 2 of a $(u, \mathbf{e}, s)$-sequence in base b is slightly stronger than Tezuka's original definition in [18], and so Tezuka's discrepancy bound is obviously valid for our concept of a $(u, \mathbf{e}, s)$-sequence in base b as well.

Our new Halton-type sequences are (t, s)-sequences in base q as well as $(u, \mathbf{e}, s)$-sequences in base q with suitable t, u, and $\mathbf{e}$. Therefore we can apply two versions of the discrepancy bound (15), namely the one with $C = C_{\text{FK}}$ and the one with $C = C_{\text{Tez}}$. It is of interest to compare these two bounds. Recall from Theorem 1 and Corollary 1 that for these sequences we have $u = g$, the genus of the global function field F, as well as $\mathbf{e} = (e_1, \ldots, e_s)$ and $t = g + \sum_{i=1}^{s}(e_i - 1)$, where $e_i = \deg(P_i)$ for $1 \leqslant i \leqslant s$. Then from (16) and (17) we obtain

$$\frac{C_{\text{FK}}}{C_{\text{Tez}}} \geqslant \frac{1}{2} \left(\frac{q-1}{q} \right)^s \prod_{i=1}^{s} e_i.$$

Thus, if

$$(18) \qquad \prod_{i=1}^{s} e_i > 2 \left(\frac{q}{q-1} \right)^s ,$$

then the discrepancy bound with the constant C_{Tez} is better than the one with the constant C_{FK}. The condition (18) will be satisfied in many cases. For instance, it was shown in [5] that if we arrange all distinct places $\neq P_\infty$ of F into a list $P_1, P_2, \ldots$ in an arbitrary manner, then for any $0 < \varepsilon < 1/q$ we have

$$\prod_{i=1}^{s} \deg(P_i) > (\log_q s)^{((1/q) - \varepsilon)s}$$

for all sufficiently large s, where $\log_q$ denotes the logarithm to the base q. Hence in this situation the condition (18) is satisfied for all sufficiently large s, and so the discrepancy bound (15) with the constant $C = C_{\text{Tez}}$ is better than the one with $C = C_{\text{FK}}$.

The discussion above shows that the theory of $(u, \mathbf{e}, s)$-sequences is a useful extension of the theory of (t, s)-sequences since, for instance, it can lead to improved discrepancy bounds in comparison with the discrepancy bounds for (t, s)-sequences.

Acknowledgment

References

[1] Colbourn C J, Dinitz J H, eds. Handbook of Combinatorial Designs, 2nd ed. Boca Raton: CRC Press, 2006
[2] Dick J, Pillichshammer F. Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration. Cambridge: Cambridge University Press, 2010
[3] Faure H, Kritzer, P. New star discrepancy bounds for (t, m, s)-nets and (t, s)-sequences. Preprint, 2012
[4] Halton J H. On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals. Numer Math, 1960, 2: 84–90

[5] Hofer R, Niederreiter H. A construction of (t, s)-sequences with finite-row generating matrices using global function fields. Preprint, 2012; available at http://arxiv.org/abs/1210.5152

[6] Mayor D J S, Niederreiter H. A new construction of (t, s)-sequences and some improved bounds on their quality parameter. Acta Arith, 2007, 128: 177–191

[7] Niederreiter H. Point sets and sequences with small discrepancy. Monatsh Math, 1987, 104: 273–337

[8] Niederreiter H. Low-discrepancy and low-dispersion sequences. J Number Theory, 1988, 30: 51–70

[9] Niederreiter H. Random Number Generation and Quasi-Monte Carlo Methods. CBMS-NSF Regional Conference Series in Applied Math, 63. Philadelphia: Soc Industrial Applied Math, 1992

[10] Niederreiter H, Özbudak F. Low-discrepancy sequences using duality and global function fields. Acta Arith, 2007, 130: 79–97

[11] Niederreiter H, Xing C P. Low-discrepancy sequences obtained from algebraic function fields over finite fields. Acta Arith, 1995, 72: 281–298

[12] Niederreiter H, Xing C P. Low-discrepancy sequences and global function fields with many rational places. Finite Fields Appl, 1996, 2: 241–273

[13] Niederreiter H, Xing C P. Quasirandom points and global function fields. In: Cohen S, Niederreiter H, eds. Finite Fields and Applications. London Math Soc Lecture Note Series, 233. Cambridge: Cambridge University Press, 1996. 269–296

[14] Niederreiter H, Xing C P. Nets, (t, s)-sequences, and algebraic geometry. In: Hellekalek P, Larcher G, eds. Random and Quasi-Random Point Sets. Lecture Notes in Statistics, 138. New York: Springer, 1998. 267–302

[15] Niederreiter H, Xing C P. Rational Points on Curves over Finite Fields: Theory and Applications. London Math Soc Lecture Note Series, 285. Cambridge: Cambridge University Press, 2001

[16] Stichtenoth H. Algebraic Function Fields and Codes, 2nd ed. Berlin: Springer, 2009

[17] Tezuka S. Polynomial arithmetic analogue of Halton sequences. ACM Trans Modeling Computer Simulation, 1993, 3: 99–107

[18] Tezuka S. On the discrepancy of generalized Niederreiter sequences. Preprint, 2012

[19] Xing C P, Niederreiter H. A construction of low-discrepancy sequences using global function fields. Acta Arith, 1995, 73: 87–102

HARALD NIEDERREITER, JOHANN RADON INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS, AUSTRIAN ACADEMY OF SCIENCES, ALTENBERGERSTR. 69, A-4040 LINZ, AUSTRIA, AND DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SALZBURG, HELLBRUNNERSTR. 34, A-5020 SALZBURG, AUSTRIA; ANDERSON SIANG JING YEO, SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES, NANYANG TECHNOLOGICAL UNIVERSITY, 21 NANYANG LINK, NTU SPMS-MAS-04-20, SINGAPORE 637371, REPUBLIC OF SINGAPORE

E-mail address: ghnied@gmail.com (Harald Niederreiter), yeos0041@e.ntu.edu.sg (Anderson Siang Jing Yeo)